PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-233460
(43)Date of publication of application : 10.09.1993

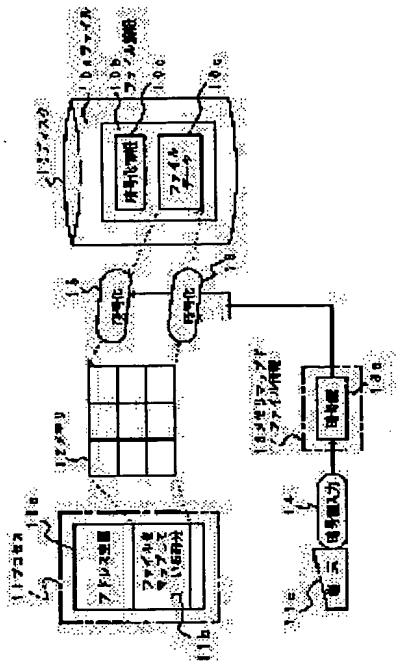
(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 04-034764
(22)Date of filing : 21.02.1992

(71)Applicant : TOSHIBA CORP
(72)Inventor : HIRAYAMA HIDEAKI

(54) FILE PROTECTION SYSTEM

(57)Abstract:
PURPOSE: To encipher a file placed on an external device at all times by providing means which decipher the data of an enciphered file among memory mapped files by using an enciphering key when the data are transferred from the external storage to a main memory and enciphers the data by using the enciphering key when the data are put back to the external storage.
CONSTITUTION: This system is equipped with a means which inputs the enciphering key from outside and records it as an enciphering key 13a in memory mapped file information 13, the deciphering means 15 which deciphers the data, block by block, by using the enciphering key 13a in the memory mapped file information 13 when the enciphered file data 10c are transferred from the disk 10 the main memory 12, and the enciphering means 16 which enciphers the file data on the main memory 12, block by block, by using the enciphering key 13a when the file data transferred to the main memory 12 are put back onto the disk 10.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平5－233460

(43)公開日　平成５年(1993) ９月10日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｂ	9293－5B		
12/00	５３７　Ｈ	7232－5B		

審査請求　未請求　請求項の数２(全 10 頁)

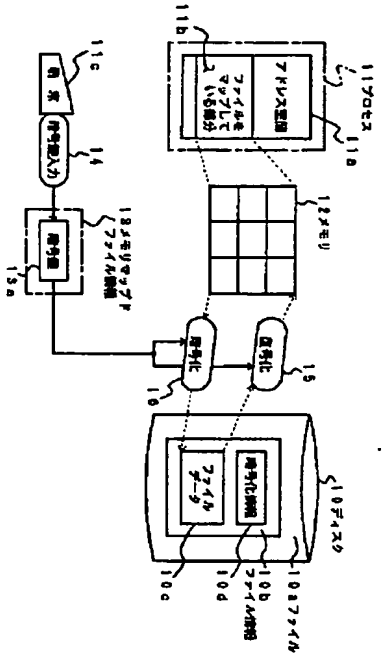
(21)出願番号　特願平4－34764

(22)出願日　平成４年(1992) ２月21日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　平山　秀昭
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　ファイル保護方式

(57)【要約】
【目的】本発明は、メモリマップドファイルに於いて、暗号化されたファイルのデータを外部記憶から主メモリに移す際に暗号鍵を用いて復号化し、そのデータを外部記憶へ戻す際に暗号鍵を用いて暗号化する手段を有して、外部記憶装置上に置かれたファイルを常に暗号化できることを最も主要な特徴とする。
【構成】暗号鍵を外部より入力しメモリマップドファイル情報１３中に暗号鍵１３ａとして記録する手段と、暗号化されたファイルデータ１０ｃをディスク１０から主メモリ１２に移す際に、同データをメモリマップドファイル情報１３中の暗号鍵１３ａを用いブロック単位で復号化する復号化手段１５と、主メモリ１２に移されたファイルデータをディスク１０に戻す際に、主メモリ１２上のファイルデータを暗号鍵１３ａを用いブロック単位で暗号化する暗号化手段１６とを具備してなることを特徴とする。



1

【特許請求の範囲】

【請求項１】　外部記憶装置上のファイルをプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、

主記憶上にマップするマップ対象ファイルが暗号化されているか否かを識別する手段と、

同手段で上記マップ対象ファイルが暗号化されていることを識別した際に外部より暗号鍵を入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、

上記暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、同データを上記保持した暗号鍵を用いて復号化する手段と、

上記主記憶上のファイルのデータを外部記憶装置に戻す際に、同データを上記保持した暗号鍵を用いて暗号化する手段とを具備してなることを特徴とするファイル保護方式。

【請求項２】　ネットワークで接続されたリモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、

上記マップの対象となるファイルが暗号化されているか否かを識別する手段と、

同手段で上記マップの対象となるファイルが暗号化されていることを識別した際に暗号鍵を外部より入力し、対応するファイルがマップされている間、上記暗号鍵を保持する手段と、

上記暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後、同データを上記保持された暗号鍵を用いて復号化する手段と、

上記復号されたファイルのデータをローカル電子計算機からリモート電子計算機に戻す際に同データを上記保持された暗号鍵を用いて暗号化する手段とを具備してなることを特徴とするファイル保護方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、機密性の高いファイルを扱う電子計算機システムに適用して好適な、ファイルの情報漏洩を防ぐためのファイル保護方式に係り、特に、メモリマップドファイルの技術を用いて、機密性の高いファイルデータの高速アクセスとファイル保護を同時に実現可能にしたファイル保護方式に関する。

【０００２】

【従来の技術】近年、電子計算機システムは企業情報システムの構築に必須であり、かつ機密性の高い重要情報を保持する機会が益々増えている。社会構造が電子計算機への依存度を高めるにつれ、ハッカー、ウイルス等のコンピュータ犯罪が増えている。このため機密性の高いファイルの情報保護が、強く望まれている。その一方に於いて電子計算機はその用途を益々広げ、高速処理への

2

要求が止むことはない。

【０００３】そのため近年のメモリ価格の低下を利用して、ファイルをアドレス空間上に直接マップすることにより、高速なファイルアクセスを可能にする、メモリマップドファイルの技術が重視されている。

【０００４】機密性の高いファイルを保護するためには、ファイルを暗号化しておく必要があり、ファイルを高速にアクセスするためには、上記メモリマップドファイルの技術を利用する必要がある。

【０００５】しかし暗号化されたファイルを直接にメモリマップドファイルの技術を用いてアクセスすることはできず、暗号化されたファイルを格納した外部記憶上（ディスク上）にて一旦、復号化したファイルを作成し、そのファイルをメモリマップドファイルの技術を用いて、アクセスしなければならなかった。そのため結局のところ機密性の高いファイルが暗号化されない形でディスク上に存在してしまい、情報漏洩の危機に曝されてしまうという問題があった。

【０００６】

【発明が解決しようとする課題】上記したように従来のファイル保護方式は、ファイルを高速にアクセスするためのメモリマップドファイルの技術とは相容れないもので、従来のファイル保護方式をメモリマップドファイルの技術に適用することは困難であり、結局のところ機密性の高いファイルが暗号化されない形でディスク上に存在してしまい、情報漏洩の危機に曝されてしまうという問題があった。

【０００７】本発明は上記実情に鑑みなされたもので、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、ファイルを高速にアクセスすることにより、ファイルの保護と高速処理を同時に実現することができるファイル保護方式を提供することを目的とする。

【０００８】

【課題を解決するための手段】本発明のファイル保護方式は、外部記憶装置上のファイルをプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするマップ対象ファイルが暗号化されているか否かを識別する手段と、同手段でマップ対象ファイルが暗号化されていることを識別した際に暗号鍵を外部より入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、上記保持した暗号鍵を用いて、上記データを上記各記憶装置間のデータ交換単位をもとに設定された所定のデータ量単位、例えばブロック単位で復号化する手段と、上記主記憶上のファイルのデータを外部記憶装置に戻す際に、上記保持した暗号鍵を用いて、上記データをブロック単位で暗号化する手段とを具備してなることを特徴とする。

3

【０００９】又、本発明のファイル保護方式は、ネットワークで接続されたリモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするファイルが暗号化されているか否かを識別する手段と、同手段でファイルが暗号化されていることを識別した際に暗号鍵を入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後、上記保持された暗号鍵を用いて上記データをブロック単位で復号化する手段と、上記復号化されたファイルのデータをローカル電子計算機からリモート電子計算機に戻す際に上記保持された暗号鍵を用いてデータをブロック単位で暗号化する手段とを具備したことを特徴とする。

【００１０】

【作用】上記構成に於いて、暗号化されているファイルを主記憶上にマップする際は、外部から暗号鍵情報を入力し、メモリマップドファイル情報中に暗号鍵として記録する。その後、暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、その暗号化されたファイルのデータを上記メモリマップドファイル情報中に含まれる暗号鍵を用いブロック単位で復号化する。又、主記憶上のファイルのデータを外部記憶装置に戻す際に、そのファイルのデータを上記暗号鍵を用いブロック単位で暗号化する。これにより外部記憶装置に格納されるファイルは常に暗号化されたファイルデータであり、従って、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理が同時に実現可能となる。

【００１１】又、本発明のファイル保護方式に於いては、ネットワークで接続されたリモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップして、ファイルを直接アクセスするメモリマップドファイル機構に於いても適用され、この際は、ローカル電子計算機の主記憶上にマップするファイルが暗号化されているとき、その暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後に、外部より入力された暗号鍵を用いて上記データをブロック単位で復号化する。又、ローカル電子計算機の主記憶上のファイルのデータをローカル電子計算機からリモート電子計算機に戻す際は、そのファイルのデータを上記暗号鍵を用いブロック単位で暗号化し、リモート電子計算機に戻す。このように、暗号化されているデータは、ネットワークを経由して転送した後に復号化され、又、復号化されているデータは、ネットワークを経由して転送する前に暗号化されることにより、ネットワーク上を転送しているデータからの情報漏洩を防ぐことができる。又、リモート電子計算機のファイルメモリ（外部記憶装置）上に於いては、常に暗号化されたファイルデータのみが格納される。従って、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理が同時に実現される。

4

【００１２】

【実施例】以下図面を参照して本発明の一実施例を説明する。図１は本発明の一実施例の構成を示すブロック図である。ここでは、外部記憶装置となるディスク１０上のファイル１０ａをプロセス１１のアドレス空間１１ａの部分１１ｂにマップしている。上記ファイル１０ａは、ファイル情報１０ｂと、ファイルデータ１０ｃより構成される。ファイル情報１０ｂ中には、ファイルデータ１０ｃが暗号化されているか否かを示す暗号化情報１０ｄが含まれる。

【００１３】暗号化されているファイルを主メモリ１２上にマップしようとした場合は、端末装置１１ｃから暗号鍵を入力し、得られた暗号鍵情報をメモリマップドファイル情報１３中に暗号鍵１３ａとして記録する。

【００１４】尚、暗号鍵を入力する端末装置としては、ユーザの端末装置の他に、オペレータコンソール等も考えられる。また暗号鍵は、端末装置以外の装置から入力することも可能であり、例えばプログラム中に暗号鍵を埋め込む等も考えられる。

【００１５】主メモリ１２上にマップされたファイルをプロセス１１がアクセスし、暗号化されているファイルデータ１０ｃをディスク１０から主メモリ１２に移す場合には、その暗号化されているファイルデータ１０ｃを上記メモリマップドファイル情報１３中の暗号鍵１３ａを用いてブロック単位で復号化する。

【００１６】即ち、主メモリ１２上にマップするファイルのデータが暗号化されている（マップ対象ファイルのファイル情報１０ｂに含まれる暗号化情報１０ｄが、ファイル情報１０ｂの暗号化されていることを示している）際は、その暗号化されたファイルデータ１０ｃをディスク１０から主メモリ１２に移す際に、そのデータが、復号化手段１５により、メモリマップドファイル情報１３中の暗号鍵１３ａを用いブロック単位で復号化される。

【００１７】また逆に、ディスク１０から主メモリ１２に移されていた復号化されたデータを、再びディスク１０に戻す場合も同データを上記暗号鍵１３ａを用いてブロック単位で暗号化する。

【００１８】即ち、上記復号化手段１５により復号化され主メモリ１２に移されたファイルデータをディスク１０に戻す際は、主メモリ１２上のファイルデータが暗号化手段１６により上記暗号鍵１３ａを用いてブロック単位で暗号化される。図２は上記図１に示す実施例に於い

て、暗号化されているファイルを主メモリ１２上にマッピングするマッピング処理の流れを示すフローチャートである。

【００１９】図２に於いて、Ａ１は主メモリ１２上にマップするファイルが暗号化されているか否かを調べる判断ステップである。ここで暗号化されていることを判断すると、ステップＡ２，Ａ３の処理を行なってからステップＡ４の処理を行なう。また、暗号化されていない場合は、ステップＡ２，Ａ３の処理は行なわず、ステップＡ４の処理を行なう。

【００２０】Ａ２は暗号鍵１３ａを入力する処理ステップ、Ａ３は入力された暗号鍵１３ａをメモリマップドファイル情報１３中に記録する処理ステップである。Ａ４は通常のメモリマップドファイルのマッピング処理を行う処理ステップである。

【００２１】図３は上記図１に示す実施例に於いて、主メモリ１２上にマッピングされた暗号化ファイルのデータをディスク１０から主メモリ１２上に移す処理（メモリマップドファイルのページイン処理）の流れを示すフローチャートである。

【００２２】図３に於いて、Ｂ１は主メモリ１２上にマップされたファイルのページをディスク１０から主メモリ１２に移すステップである。Ｂ２は主メモリ１２上にマップされたファイルのデータが暗号化されているか否かを調べる判断ステップである。

【００２３】ここで、上記マップされたファイルのデータが暗号化されているときは、ステップＢ３の処理を行なってからステップＢ４の処理を行なう。又、上記マップされたファイルのデータが暗号化されていないときは、ステップＢ３の処理は行なわずにステップＢ４の処理を行なう。

【００２４】Ｂ３はディスク１０から主メモリ１２に移すページ中のデータを暗号鍵１３ａを用いて復号化する処理ステップであり、Ｂ４は通常のメモリマップドファイルのページイン処理を行なう処理ステップである。

【００２５】図４は上記図１に示す実施例に於いて、主メモリ１２上にマッピングされている暗号化ファイルのデータを主メモリ１２からディスク１０に戻す処理（メモリマップドファイルのページアウト処理）の流れを説明するフローチャートである。図４に於いて、Ｃ１は主メモリ１２上にマップされているファイルが暗号化するファイルのデータであるか否かを調べる処理ステップである。

【００２６】ここで暗号化するファイルのデータであるときは、ステップＣ２の処理を行なってからステップＣ３，Ｃ４の処理を行なう。又、暗号化しないファイルのデータであるときはステップＣ２の処理を行なわずにステップＣ３，Ｃ４の処理を行なう。

【００２７】Ｃ２は主メモリ１２からディスク１０に戻すページ中のデータを暗号鍵１３ａを用いて暗号化する処理ステップであり、Ｃ３は主メモリ１２上にマップされたファイルのページをディスク１０に戻すステップである。Ｃ４は通常のメモリマップドファイルのページアウト処理を行なう処理ステップである。

【００２８】上記図１乃至図４に示す実施例に於いて、ディスク１０上の暗号化されているファイルを主メモリ１２上にマップする際は、端末装置１１ｃから暗号鍵を入力し、その入力された暗号鍵情報をメモリマップドファイル情報１３中に暗号鍵１３ａとして記録する。

【００２９】即ち、この際の暗号化されているファイルを主メモリ１２上にマッピングするマッピング処理では、主メモリ１２上にマップするファイルが暗号化されているか否かを調べる（図２ステップＡ１）。

【００３０】この際、主メモリ１２上にマップするファイルのファイル情報１０ｂに含まれる暗号化情報１０ｄは、該当ファイル情報１０ｂが暗号化されているか否かを示している。

【００３１】ここで、主メモリ１２上にマップするファイルのデータが暗号化されている際は、暗号鍵を入力する処理で入力された暗号鍵情報を暗号鍵１３ａとしてメモリマップドファイル情報１３中に記録（図２ステップＡ２，Ａ３）した後、通常のメモリマップドファイルのマッピング処理を行なう（図２ステップＡ４）。

【００３２】又、主メモリ１２上にマップするファイルのデータが暗号化されていない際は、上記暗号鍵の処理（図２ステップＡ２，Ａ３）を行なわずに、通常のメモリマップドファイルのマッピング処理を行なう（図２ステップＡ４）。

【００３３】上記マッピング処理により主メモリ上にマップされたファイルをプロセス１１がアクセスし、そのファイルのデータをディスク１０から主メモリ１２に移す際は、該当ファイルデータ１０ｃが暗号化されていれば、その暗号化されているファイルデータ１０ｃが上記メモリマップドファイル情報１３中の暗号鍵１３ａを用いて復号化される。

【００３４】即ち、ディスク１０上のファイルデータを主メモリ１２に移す際は、ディスク１０より読出されるファイルのデータが暗号化されているか否かが判断される（図３ステップＢ１）。

【００３５】ここで、主メモリ上にマップされたファイルのデータが暗号化されている際は、その暗号化されたファイルデータ１０ｃをディスク１０から主メモリ１２上に移す際に、そのデータが、復号化手段１５により、メモリマップドファイル情報１３中の暗号鍵１３ａを用いブロック単位で復号化され（図３ステップＢ２，Ｂ３）、その復号化処理を介在して、メモリマップドファイルのページイン処理が行なわれる（図３ステップＢ４）。

【００３６】次に、ディスク１０から主メモリ１２上に移されている、復号化されたデータをディスク１０に戻

す場合も、その復号化されたデータが上記暗号鍵１３ａを用いて暗号化される。

【００３７】即ち、主メモリ１２のファイルデータをディスク１０に戻す際は、主メモリ１２上にマップされているファイルが暗号化するファイルのデータであるか否かが判断される（図４ステップＣ１）。

【００３８】ここで、暗号化するファイルのデータであるときは、主メモリ１２からディスク１０に戻すページ中のデータが暗号化手段１６により暗号鍵１３ａを用いて暗号化され（図４ステップＣ２，Ｃ３）、その暗号化処理を介在して、メモリマップドファイルのページアウト処理が行なわれる（図４ステップＣ４）。

【００３９】このようなファイルの処理制御により、暗号化されたファイルはディスク１０上では復号化されることがなく、従って「トロイの木馬」のような手法（ファイルとして見えても真のデータは隠されている状態）により、ファイル自体が不正コピー等により盗難されたとしても、暗号鍵の盗難がない限り、機密情報の漏洩を防止することができる。

【００４０】また主メモリ１２上にマップされたファイルのページイン／ページアウト処理が頻発すると、ファイルデータの暗号化／復号化のオーバヘッドが増加するが、近年はメモリ価格が低下しているので、大容量のメモリを使用することにより、この問題は解消される。図５は本発明の他の実施例を示すブロック図である。

【００４１】ここでは、リモートノード２８上のディスク２０に格納されたファイル２０ａを、ローカルノード２７上のプロセス２１のアドレス空間２１ａの部分２１ｂにマップする例を示している。この際、上記ファイル２０ａはファイル情報２０ｂとファイルデータ２０ｃより構成されるものとする。ファイル情報２０ｂ中には暗号化情報２０ｄが含まれていて、ファイルデータ２０ｃが暗号化されているか否かを示している。

【００４２】暗号化されているファイルをメモリ２２上にマップしようとした場合は、端末装置２１ｃに対して暗号鍵を要求し、得られた暗号鍵情報をメモリマップドファイル情報２３中に、暗号鍵２３ａとして記録する。２９はローカルノード２７とリモートノード２８が通信を行なうためのネットワークである。

【００４３】メモリ２２上にマップされたファイルをプロセス２１がアクセスし、暗号化されているファイルデータをネットワーク２９を経由して、リモートノード２８のディスク２０からローカルノード２７のメモリ２２に移す場合には、ファイルデータ２０ｃがネットワーク２９を経由してローカルノード２７に送られた後に、復号化手段２５により暗号鍵２３ａを用いてブロック単位で復号化される。

【００４４】また、これとは逆に、リモートノード２８のディスク２０からローカルノード２７のメモリ２２に移されていたデータをネットワーク２９を経由して再び

リモートノード２８のディスク２０に戻す場合には、そのファイルデータをネットワーク２９を経由してリモートノード２８に送る際に、暗号化手段２６により暗号鍵２３ａを用いてブロック単位で再び暗号化される。

【００４５】このように、暗号化されているデータは、ネットワーク２９を経由して転送した後に復号化され、又、復号化されているデータは、ネットワーク２９を経由して転送する前に暗号化されることにより、ネットワーク２９上を転送しているデータからの情報漏洩を防ぐことができる。

【００４６】

【発明の効果】以上詳記したように本発明のファイル保護方式によれば、外部記憶装置上のファイルをプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするマップ対象ファイルが暗号化されているか否かを識別する手段と、同手段でマップ対象ファイルが暗号化されていることを識別した際に暗号鍵を外部より入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータを外部記憶装置から主記憶上に移す際に、上記保持した暗号鍵を用いて、上記データを所定のデータ転送単位（例えばブロック単位）で復号化する手段と、上記主記憶上のファイルのデータを外部記憶装置に戻す際に、上記保持した暗号鍵を用いて、上記データをブロック単位で暗号化する手段とを具備してなる構成としたことにより、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理を同時に実現できる。

【００４７】又、本発明のファイル保護方式によれば、ネットワークで接続されたリモート電子計算機上のファイルをローカル電子計算機上のプロセスのアドレス空間上にマップし、プログラムからファイルを直接アクセスするメモリマップドファイルに於いて、主記憶上にマップするファイルが暗号化されているか否かを識別する手段と、同手段でファイルが暗号化されていることを識別した際に暗号鍵を入力し、対応ファイルがマップされている間、上記暗号鍵を保持する手段と、上記暗号化されたファイルのデータをリモート電子計算機からローカル電子計算機に移した後、上記保持された暗号鍵を用いて上記データをブロック単位で復号化する手段と、上記復号されたファイルのデータをローカル電子計算機からリモート電子計算機に戻す際に上記保持された暗号鍵を用いてデータをブロック単位で暗号化する手段とを具備してなる構成としたことにより、暗号化されているデータは、ネットワークを経由して転送した後に復号化され、又、復号化されているデータは、ネットワークを経由して転送する前に暗号化されることから、ネットワーク上を転送しているデータからの情報漏洩を防ぐことができ

9

る。又、リモート電子計算機のファイルメモリ（外部記憶装置）上に於いては、常に暗号化されたファイルデータのみが格納されることから、機密性の高いファイルを暗号化したまま、復号化コピーを作ることなく、メモリマップドファイルの技術を用いて、高速にアクセスすることができ、ファイルの保護と高速処理が同時に実現できる。

【図面の簡単な説明】

【図１】本発明の一実施例の構成を示すブロック図。

【図２】図１の実施例に於いて、暗号化されたファイルをメモリ上にマッピングする処理を説明するためのフローチャート。

【図３】図１の実施例に於いて、メモリ上にマップされた暗号化対象ファイル中のデータをディスクからメモリに移す処理を説明するためのフローチャート。

【図４】図１の実施例に於いて、メモリ上にマップされた暗号化ファイル中のデータを、メモリからディスクに

10

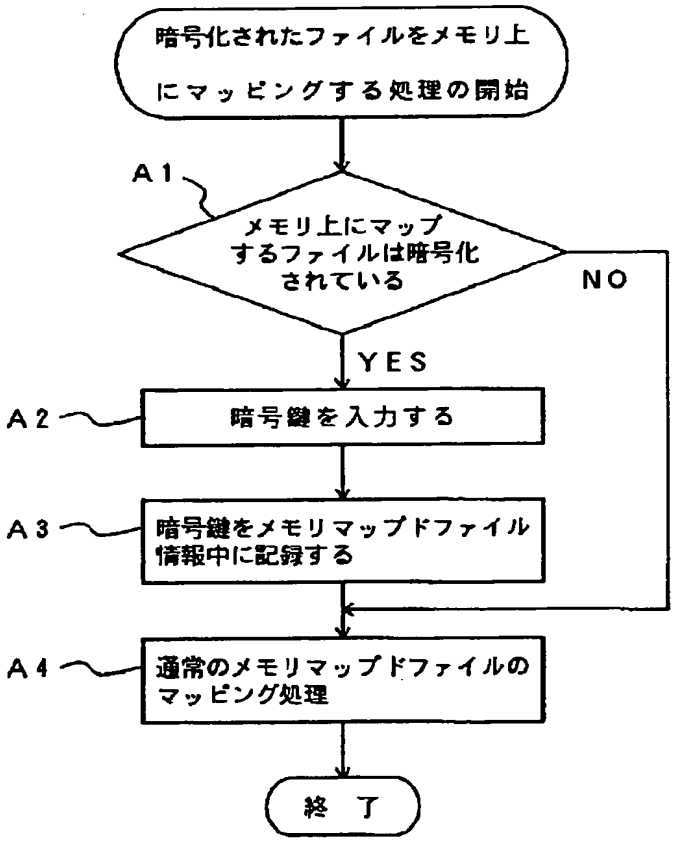
戻す処理を説明するためのフローチャート。

【図５】本発明の他の実施例の構成を示すブロック図。

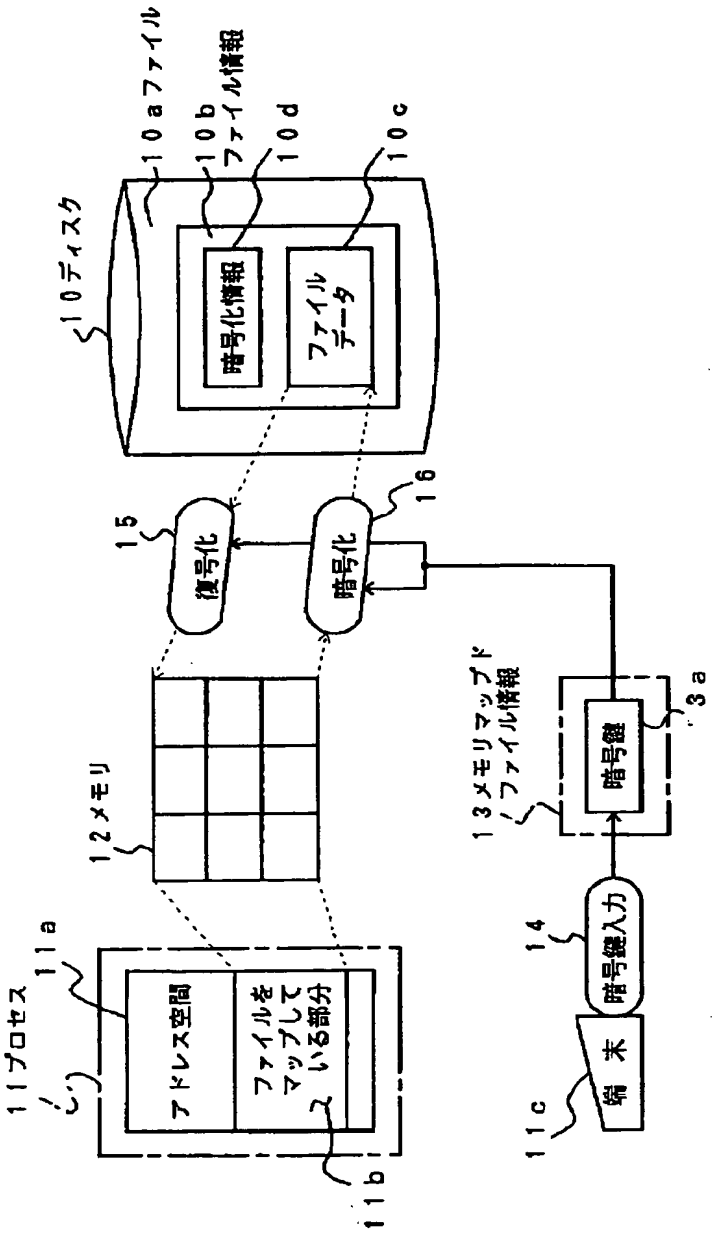
【符号の説明】

１０…ディスク、１０ａ…ファイル、１０ｂ…ファイル情報、１０ｃ…ファイルデータ、１０ｄ…暗号化情報、１１…プロセス、１１ａ…アドレス空間、１１ｂ…ファイルをマップしている部分、１１ｃ…端末装置、１２…メモリ、１３…メモリマップドファイル情報、１３ａ…暗号鍵、１４…暗号鍵入力手段、１５…復号化手段、１６…暗号化手段、２０…ディスク、２０ａ…ファイル、２０ｂ…ファイル情報、２０ｃ…ファイルデータ、２０ｄ…暗号化情報、２１…プロセス、２１ａ…アドレス空間、２１ｂ…ファイルをマップしている部分、２１ｃ…端末装置、２２…メモリ、２３…メモリマップドファイル情報、２３ａ…暗号鍵、２４…暗号鍵入力手段、２５…復号化手段、２６…暗号化手段、２７…ローカルノード、２８…リモートノード、２９…ネットワーク。

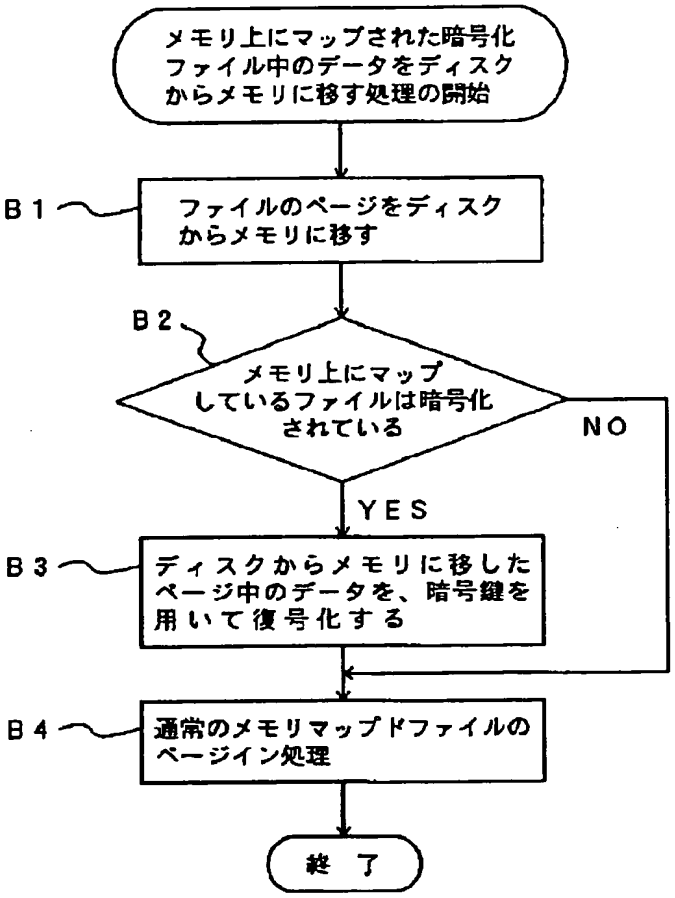
【図２】



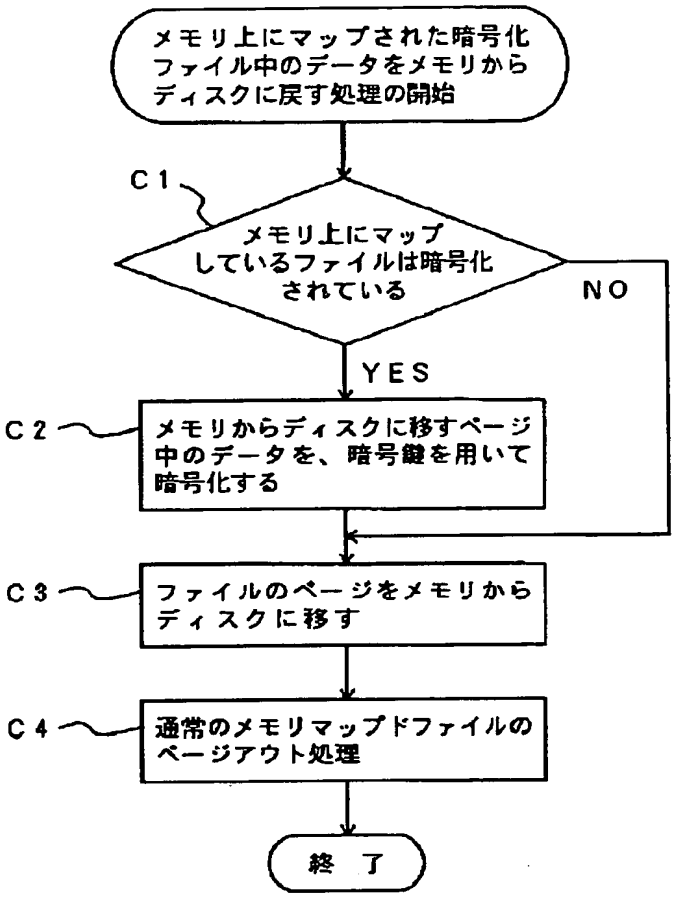
【図1】


10ディスク
10aファイル
10bファイル情報
10d
10c
暗号化情報
ファイルデータ
15
復号化
16
暗号化
12メモリ
13メモリマップドファイル情報
暗号鍵
3a
14
暗号鍵入力
端末
11c
11プロセス
11a
アドレス空間
ファイルをマップしている部分
11b

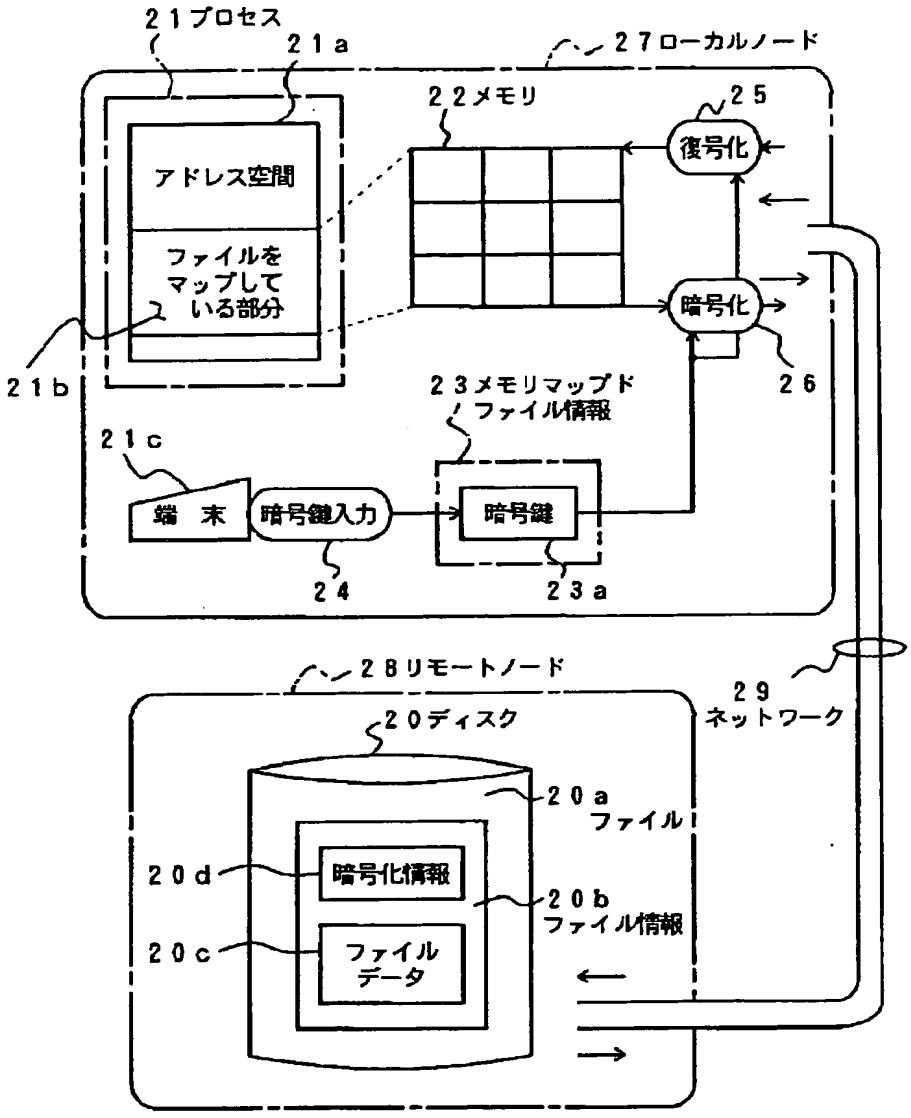
【図3】


メモリ上にマップされた暗号化ファイル中のデータをディスクからメモリに移す処理の開始
B1
ファイルのページをディスクからメモリに移す
B2
メモリ上にマップしているファイルは暗号化されている
NO
YES
B3
ディスクからメモリに移したページ中のデータを、暗号鍵を用いて復号化する
B4
通常のメモリマップドファイルのページイン処理
終了

【図4】


メモリ上にマップされた暗号化ファイル中のデータをメモリからディスクに戻す処理の開始
C1
メモリ上にマップしているファイルは暗号化されている
NO
YES
C2
メモリからディスクに移すページ中のデータを、暗号鍵を用いて暗号化する
C3
ファイルのページをメモリからディスクに移す
C4
通常のメモリマップドファイルのページアウト処理
終　了

【図５】


２１プロセス
２１ａ
２７ローカルノード
２２メモリ
２５
復号化
アドレス空間
ファイルを
マップして
いる部分
暗号化
２１ｂ
２６
２３メモリマップド
ファイル情報
２１ｃ
端　末
暗号鍵入力
暗号鍵
２４
２３ａ
２８リモートノード
２９
ネットワーク
２０ディスク
２０ａ
ファイル
２０ｄ
暗号化情報
２０ｂ
ファイル情報
２０ｃ
ファイル
データ